



(19)

Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 1 330 073 A1

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:
23.07.2003 Bulletin 2003/30(51) Int Cl.7: H04L 12/28, H04Q 7/38,
H04Q 7/22

(21) Application number: 02250352.8

(22) Date of filing: 18.01.2002

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE TRDesignated Extension States:
AL LT LV MK RO SI(71) Applicant: Nokia Corporation
02150 Espoo (FI)

- Smith, Mike P.
Cambridge, CB4 5JB (GB)
- Takamäki, Timo
33720 Tampere (FI)
- Tuomi, Jukka
33730 Tampere (FI)
- Tuominen, Hannu
02700 Kauniainen (FI)

(72) Inventors:

- Haverinen, Henry
33720 Tampere (FI)
- Bush, Anton
Nottingham NG9 2EZ (GB)
- Rinnemaa, Jyri
33820 Tampere (FI)

(74) Representative:
Pitkänen, Hannu Alpo Antero et al
Patent Agency Pitkänen Oy,
P.O. Box 1188
70211 Kuopio (FI)

(54) Method and apparatus for access control of a wireless terminal device in a communications network

(57) A method and device for routing data packets (110) of a wireless terminal device in a communication network. When Open system Authentication is used (103) the system operates similarly as the current Nokia Operator Wireless LAN system, in which the terminal device and the access controller are the parties involved in the authentication (105). The access controller relays information relating to the authentication between the terminal device and an authenticating server, and it is capable of updating independently the list of users it maintains. When authentication according IEEE 802.1X authentication (102), the access point operates according to the IEEE 802.1X standard (108), serving as the authenticating party and relaying information relating to the authentication between the terminal device and the authentication server. In addition, the list maintained by the access controller is updated (107) after a successful authentication, for example by the access point or the authenticating server.

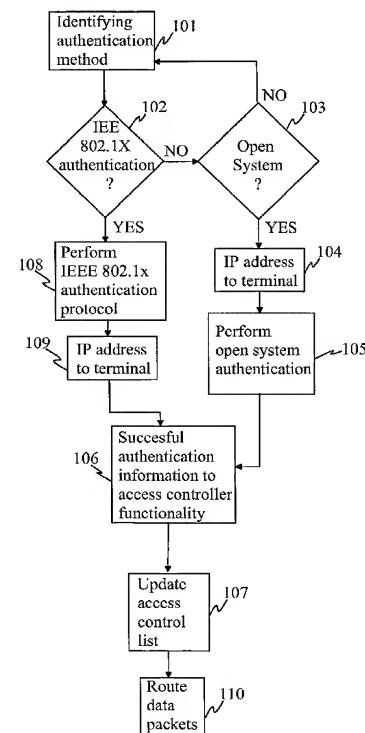


Fig. 1

Description

[0001] The present invention relates to a method and apparatus for access control of a wireless terminal device to a communications network and particularly, although not necessarily, for relaying data packets of a wireless terminal device having controlled access to a wireless local area network.

PRIOR ART

[0002] A wireless local area network typically comprises a network comprising terminal devices, such as wireless terminal devices or portable computers and access points, wherein data transmission between the terminal devices and the access points is carried out partly or entirely in a wireless manner using radio waves or infrared technology.

[0003] The structure of telecommunications networks is generally described using the OSI model (Open System Interconnection), which defines the interfaces through which the different devices and the related software communicate with each other. The OSI model is based on a concept of layers, the lowest, or first, layer being known as a Physical Layer encompassing all logical, electrical and mechanical issues relating to data transfer. The second protocol layer, i.e. the Data Link Layer, is responsible for connection set-up, error correction and connection release. The third protocol layer, i.e. the Network Layer, provides data transfer not dependent on the network structure. The subsequent layers are the Transport Layer (fourth layer), Session Layer (fifth layer), Presentation Layer (sixth layer), and Application Layer (seventh layer).

[0004] In the OWLAN (Operator Wireless Local Area Network) system, authentication and access control currently take place on the third layer of the OSI model, i.e. the network layer, or IP layer, and WLAN-association between the terminal device and the Access Point is carried out without authentication. An access point is a physical device, such as a base station, interconnecting a wireless network and a wired one. In Open System Authentication the association event does not involve actual authentication, but the open system authentication, performed before association, is null authentication. After the association, the terminal device is typically provided with an IP address after the association event by means of an IP-based DHCP (Dynamic Host Configuration Protocol) method. Authentication is then carried out by executing an IP-based authentication protocol. Although the authentication protocol also employs protocol layers above the IP layer, the authentication is in this case referred to as authentication of the third protocol layer because access control is typically implemented on the third protocol layer. The Operator Wireless LAN solution includes the Network Access Authentication Protocol (NAAP), which is a protocol of the third protocol layer to authenticate the wireless terminal using

the GSM Subscriber Identity Module. Another example of a third protocol layer authentication protocol are solutions based on the Hypertext Transfer Protocol (HTTP), where the authentication is performed using a World Wide Web (WWW) page in which the user fills in the credentials. Yet another example of a third protocol layer authentication protocol is the Internet Key Exchange (IKE) Protocol, which is used when setting up a Virtual Private Network connection. In all these examples, the wireless terminal needs to perform the third protocol layer authentication protocol before it can access the resources for which access control is being enforced.

[0005] Standardization provides a framework for hardware and software manufacturers to enable products of different manufacturers to be used side by side. The title of the WLAN standard is IEEE 802.11 and it has gradually been supplemented by a number of sub-standards. According to the forthcoming IEEE 802.11i standard, WLAN authentication will be carried out according to a second protocol layer authentication method, such as an IEEE802.1x protocol before transmission of IP packets between the terminal device and the network.

[0006] The first router in the OWLAN system, i.e. the edge router, which is between the communications network and the wireless terminals connected to the wireless local area network, functions in the OWLAN as the other party in the authentication carried out according to the third protocol layer, i.e. open system authentication and it maintains an Access Control List (ACL) of authenticated terminal devices. The IEEE is standardizing a new WLAN authentication system where authentication is performed against the Access Point. If the access network deploys only the new WLAN authentication system then the present OWLAN system, such as Nokia Operator Wireless LAN Release 1.0 solution cannot be used, because the client is not allowed to run the authentication protocol of the third protocol layer without first authenticating according to IEEE 802.1x protocol.

As some users will acquire new terminal devices while others will have old terminal devices, there will be "old" terminals that can access to the network by using the third protocol layer authentication method and further there will be "new" terminals that can access to the network by using the authentication method according to IEEE 802.1x standard. Also there will be networks comprising access points that operate only according to IEEE 802.1x standard and other access points that operate as part of an OWLAN system. A problem that will be faced with in the standardization of current systems is the incompatibility of the present open system and the future second protocol layer authentication systems, i.e. the present terminals cannot access to networks according to the IEEE 802.1x standard and the future terminals according to the IEEE802.1x standard cannot access to the present open system networks.

SUMMARY OF THE INVENTION

[0007] A method and apparatus has now been invented for allowing a wireless terminal to access to a network by using either a third protocol layer authentication, such as open system authentication or second protocol layer authentication, such as according to the IEEE 802.1x protocol. An Access Point of the invention enables both Open System Authentication, in which the terminal device is authenticated at a later stage according to the third protocol layer, and authentication of the second protocol layer, such as IEEE 802.1x authentication. By using the invention certain network elements of the Wireless LAN solution can support both the new IEEE 802.1x layer 2 authentication standard and the current layer 3 authentication in a backward compatible way.

[0008] In the current Nokia Operator Wireless LAN solution, the access controller is responsible for maintaining an access control list and for performing a third protocol layer authentication protocol. In the present invention, these functionalities are separated into a logical access controller functionality and an authentication agent functionality for performing a third protocol layer authentication protocol. The network is organised so that at least part of the packets of terminal devices traverse the network element that contains the logical access controller functionality. The authentication agent functionality refers to the third protocol layer authentication protocol implementation, such as the NAAP protocol, the HTTP (Hypertext Transfer Protocol) authentication protocol or Internet Key Exchange (IKE) protocol implementation. The access controller functionality and the authentication agent functionality are not necessarily implemented in the same physical network element, but it is possible to implement the access controller functionality in the access point device or some other device instead.

[0009] If third protocol layer authentication is used, then the authentication agent operates as the authenticator entity performing the third protocol layer authentication protocol, as in the current Nokia Operator Wireless LAN solution. A successful authentication results in the terminal being added to an access control list. If the access controller functionality resides in a device separate from the authentication agent, then the authentication agent sends the terminal's information to the network element containing the access controller functionality. An authenticator is an entity that facilitates the network access authentication of the terminal device by operating as the peer entity in the authentication protocol used between the terminal and the authenticator. An authentication server is an entity that provides an authentication service to an authenticator. This service determines, from the credentials provided by the supplicant i.e. the terminal device, whether the supplicant is authorized to access the services provided by the authenticator. If second protocol layer authentication is performed, then the Access Point will first operate as

specified in the IEEE standards and operate as the Authenticator entity. In addition, after successful authentication, the Access Point updates the access control list so that the packets of the clients authenticated at the second protocol layer are relayed too. If the access controller functionality resides in a device separate from the access point, then the access point sends the terminal's information to the network element containing the access controller functionality.

[0010] The invention provides a solution that allows a wireless local area network system, such as the Nokia Operator Wireless LAN, to support both an authentication standard of the second protocol layer, i.e. Layer 2, such as an authentication standard according to the IEEE 802.1x, and the current authentication standard based on the third protocol layer, i.e. Layer 3.

[0011] When Open System Authentication is used, the system operates similarly as the current Nokia Operator Wireless LAN system, in which the terminal device and the authentication agent are the parties involved in the authentication. The authentication agent relays information relating to the authentication between the terminal device and an authenticating server, and it is capable of updating the list of authenticated users, regardless of which network element maintains the list.

[0012] When authentication according to the second protocol layer is to be carried out, such as IEEE 802.1x authentication, the access point operates according to the IEEE 802.1x standard, serving as the authenticating party and relaying information relating to the authentication between the terminal device and the authentication server. In addition, the access control list is updated after a successful authentication, for example by the access point or the authenticating server, to allow the network element that contains the access controller functionality to also relay packets of terminals authenticated according to the second protocol layer.

[0013] As regards terminals employing the second protocol layer authentication, in the implementation according to the invention the interface provided between the terminal and the network is in full accordance with the standard. The invention does not set any new requirements on terminals employing the third protocol layer authentication either.

[0014] The advantages of the invention include compatibility with the current open system, where authentication is carried out on the third protocol layer, and with a system where authentication is carried out on the second protocol layer, for example according to the IEEE 802.1x standard. Regardless of the authentication method, the network element that contains the access controller functionality is capable of carrying out the bookkeeping and accounting routines relating to the transfer of data packets. Further the devices according

[0015] According to a first aspect of the invention a method is provided for access control of a wireless ter-

terminal device in a communication network, the network comprising an access point for setting up a communication connection to the terminal device, an authentication agent for relaying authentication information between the terminal device and an authentication server, a logical access controller functionality for relaying data packets of the authenticated terminal device and blocking data packets of unauthenticated terminal devices, the logical access controller functionality further comprising a list of authenticated terminal devices, an authenticating server for providing an authenticating service for the terminal device to authenticate to the network, the terminal device being configured to use one of the following authentication methods in order to authenticate itself to the network: a first authentication method wherein the access point relays authentication information between the terminal device and the authentication server, a second authentication method wherein the authentication agent relays authentication information between the terminal device and the authentication server, characterized by the method comprising the steps of identifying at the access point whether the terminal is using the first or the second authentication method, whereby if the terminal authenticates by using the first authentication method, performing the steps of: the access point relaying authentication information between the terminal device and the authentication server, the access point sending the identifier data of the terminal device, in response to successful authentication, to the list of the access controller functionality, the access controller functionality adding the identifier data of the authenticated terminal device to the list and relaying data packets of the terminal device included on the list, and if the terminal device authenticates by using the second authentication method, performing the steps of: the access point relaying information between the terminal device and the authenticating agent, the authentication agent relaying authentication information between the terminal device and the authentication server, the authentication agent sending identifier data of the terminal device, in response to successful authentication, to the list of the access controller functionality and the access controller functionality adding the identifier data of the authenticated terminal device to the list and relaying data packets of the terminal device included on the list.

[0016] According to a second aspect of the invention an access point is provided for setting up a communication connection to a terminal device in a network, said network further comprising an authentication agent for relaying authentication information between the access point and an authentication server, a logical access controller functionality for relaying data packets of the authenticated terminals included on a list and blocking data packets of unauthenticated terminals, an authenticating server for providing an authenticating service for the terminal device to authenticate to the network, the terminal device being configured to use one of the following authentication methods in order to authenticate itself to

the network: a first authentication method wherein the access point is configured to relay authentication information between the terminal device and the authentication server, a second authentication method wherein the

- 5 access point is configured to relay authentication information between the terminal device and an authentication agent, characterized in that the access point further comprises identifying means for identifying whether the terminal device is using the first or the second authentication method, first relaying means for relaying authentication information between the terminal device and the authentication server on the basis of the identified first authentication method, sending means for sending identifier data of the terminal device, in response to successful authentication of the first authentication method, to the list of the access controller functionality, second relaying means for relaying authentication information between the terminal device and the authentication agent and sending means for sending identifier data of the terminal device, in response to successful authentication of the second authentication method, to the list of the access controller functionality.
- 10
- 15
- 20
- 25
- 30
- 35
- 40
- 45
- 50
- 55

[0017] According to a third aspect of the invention a system is provided for relaying data packets of a wireless terminal device in a communication network, the network comprising:

- the network comprising: an access point for setting up a communication connection to the terminal device in a network, said network further comprising an authentication agent for relaying authentication information between the terminal device and an authentication server, a logical access controller functionality for relaying data packets of the authenticated terminal device and for blocking data packets of unauthenticated terminal devices, the access controller further comprising a list of authenticated terminal devices and relaying means for relaying data packets of the terminal devices included on the list, an authenticating server for providing an authenticating service for the terminal device to authenticate to the network, the terminal device being configured to use one of the following authentication methods in order to authenticate itself to the network: a first authentication method wherein the access point relays authentication information between the terminal device and the authentication server, a second authentication method wherein the access controller relays authentication information between the terminal device and the authentication server, characterized in that the system comprises identifying means for identifying at the access point whether the terminal device is using the first or the second authentication method, first relaying means for relaying at the access point the authentication information of the first authentication method between the terminal device and the authentication server, second relaying means for relaying information between the terminal device and the authentication agent, third relaying means at the authentication agent for relaying authentication information of the second authentication method between the access point and the authentica-

tion server, sending means for sending from the access point identifier data of the terminal device, in response to successful authentication of the first authentication method, to the list of the access controller functionality, sending means for sending from the authentication agent the identifier data of the terminal, in response to successful authentication of the second authentication method, to the list of the access controller functionality and relaying means for relaying data packets of the terminal device included on the list.

[0018] According to a fourth aspect of the invention a method is provided for relaying data packets of a wireless terminal device in a communication network, the network comprising; an access point for setting up a communication connection to the terminal device, an access controller for relaying authentication information between the terminal device and an authentication server, an authentication server for providing an authenticating service for the terminal device to authenticate to the network, the terminal device being configured to use one of the following authentication methods in order to authenticate itself to the network: a first authentication method wherein the access point relays authentication information between the terminal device and the authentication server, a second authentication method wherein the access controller relays authentication information between the terminal device and the authentication server, the method comprising; establishing a communication connection between the terminal device and the access point, characterized by the method further comprising the steps of identifying at the access point a parameter relating to the step of establishing a communication connection, classifying the terminal device on the basis of the identified parameter and directing data packets of terminal devices of different classes to separate logical channels on the basis of the classifying.

[0019] According to a fifth aspect of the invention an access point is provided for setting up a communication connection to the terminal device in a network, said network comprising: an access controller for relaying authentication information between the terminal device and an authentication server, an authentication server for providing an authenticating service for the terminal device to authenticate to the network, the terminal device being configured to use one of the following authentication methods in order to authenticate itself to the network: a first authentication method wherein the access point relays authentication information between the terminal and the authentication server, a second authentication method wherein the access point is configured to relay authentication information between the terminal device and the access controller, said access point comprising establishing means for establishing a communication connection between the terminal device and the access point, characterized in that the access point further comprises identifying means for identifying a parameter relating to the establishment of the communica-

cation connection, classifying means for classifying the terminal device on the basis of the identified parameter and directing means for directing data packets of terminal devices of different classes to separate logical channels on the basis of the classifying.

[0020] In the following, the invention will be described in greater detail with reference to the accompanying drawings, in which

- 5 10 Figure 1 is a flow diagram illustrating a method according to an embodiment of the invention;
- 15 Figure 2 shows a device according to an embodiment of the invention;
- 15 Figure 3 shows the present Nokia Operator WLAN system;
- 20 Figure 4 shows a system according to the IEEE 802.1x protocol;
- 20 Figure 5 shows a system according to an embodiment of the invention
- 25 Figure 6 shows a flow diagram of a method according to an alternative embodiment of the invention;
- 25 Figure 7 shows an access point according to an alternative embodiment of the invention; and
- 25 Figure 8 shows a system according to an alternative embodiment of the invention.

- 30 **[0021]** Figure 1 shows a flow diagram of a method according to an embodiment of the invention. In step 101 an access point, and a terminal device, such as a wireless communications device, set up a connection and associate with each other. On the initiative of the access point, the routine then checks whether authentication according to the second protocol layer (step 102) or open system authentication according to the third protocol layer (step 103) is concerned. This check is performed at the access point based on authentication and association messages as will be explained in following. In a WLAN system according to the IEEE 802.11 standard, if the terminal is using open system authentication,
- 35 it first sends the access point an authentication request message indicating open system authentication. The access point replies with an authentication response message. The exchange of these initial authentication messages does not actually authenticate the terminal but their function is null; hence the name open system authentication. Such open system authentication is also possible in WLAN systems according to IEEE 802.11i standard. In a WLAN system according to the IEEE 802.11i standard, if the terminal is using the 802.1x authentication method, there are no initial authentication request and response messages but the terminal first associates with the access point by sending an association request to the access point. The request comprises a request to authenticate by using the authentication
- 40 method according to the IEEE 802.1x standard. Hence, the access point identifies the authentication method the terminal device is using based on the authentication and association messages. If the terminal employs the Open

system Authentication method, the terminal receives an IP address from a DHCP server, for example, which may be located at the access point, authentication agent, or elsewhere in the network (104), after which an IP-based authentication protocol according to the third protocol layer is executed (105). An IP-layer authentication is carried out between a terminal device and an authentication agent. After a successful IP-layer authentication, the authenticated terminal is updated to an access control list maintained in the network element that includes the access controller functionality (step 106 and 107). This allows the access controller to relay data packets of the terminal device. If the access controller functionality resides in the authentication agent, then the authentication agent is capable of independently updating the access control list by internally sending the terminal's identifier data to the access controller functionality. If the access controller functionality resides in some other network element than the authentication agent, then the authentication agent may update the access control list by sending a message to the network element that contains the access controller functionality. For example, this message may be sent over the IP protocol using the User Datagram Protocol (UDP). The message includes at least the identifier data of the authenticated terminal, such as an IP address of the terminal, which is to be updated in the access control list.

[0022] If the terminal device is authenticated according to the second protocol layer, the IEEE 802.1x protocol (step 102), authentication is first carried out between the terminal device and the access point (step 108). After a successful authentication according to the IEEE 802.1x protocol, the terminal receives an IP address for example from the DHCP server, which may be located for example at the access point or at the authentication agent, or elsewhere in the network (step 109), and the access point transmits information about the event to the access controller functionality (step 106). If the access point contains the access controller functionality, then the access point independently updates the access control list by internally sending the terminal's information to the access controller functionality. If the access controller functionality resides in some other network element than the access point, then the access point updates the access control list by sending a message to the network element that contains the access controller functionality. For example, this message may be sent over the IP protocol using the User Datagram Protocol (UDP). The message includes at least the identifier data of the authenticated terminal, such as an IP address or a MAC address of the terminal, which is to be updated in the access control list. The access controller functionality adds then the information, such as the IP or the MAC address of the authenticated terminal device to the list it maintains (step 107). This allows the access controller functionality to relay data packets of the terminal (step 110).

[0023] Even if the access controller functionality is

separate from the authenticator entity, such as the access point or the authentication agent, the authenticator entity does not necessarily need to send the access controller explicit information of a successful authentication

- 5 if the access controller is able to conclude it otherwise, for example in the following manner. In connection with authentication, the authenticator entity typically communicates with the authentication server, which is further inside the network. The communication usually takes place using what is known as an AAA protocol (Authentication, Authorization, Accounting), such as the RADIUS (Remote Authentication Dial In User Service) or the DIAMETER protocol. If the access controller functionality functions as RADIUS proxy server and transmits
- 10 AAA-protocol messages between the authenticator entity and the authentication server, the access controller functionality obtains information about a successful authentication already by examining the RADIUS messages. A problem that arises here in the case of IEEE
- 15 802.1x authentication is that the access controller needs the IP address of the terminal device, which is not yet known at the time the authentication succeeds, for the list it maintains. However, if the access controller functionality serves as the DHCP server distributing IP addresses after 802.1x authentication, the list can thus be updated by combining, at the access controller functionality, information about the successful authentication, the MAC address of the terminal thereby obtained, and the successful execution of the DHCP protocol, whereby an IP address corresponding to the MAC address is obtained.

- 20 **[0024]** Figure 2 shows an access point 200 of an embodiment of the invention. The access point 200 comprises a processor 201 and memory 202 for executing the operations in question and at least one application 203 for carrying out e.g. identifying of an authentication method. The access point 200 further comprises an interface 205 for connecting to the router, to servers, such as an access controller, or authentication server, for example. The access point further comprises identifying means 207 for identifying whether the terminal device is using the first or the second authentication method. Preferably the access point identifies the authentication method by receiving a message from the terminal, said message indicating the authentication method the terminal is using. If the terminal employs the open system authentication method, the message is preferably an authentication request message according to the IEEE 802.11 standard, said authentication request message indicates open system authentication. If the terminal employs the IEEE 802.1x authentication method, the message is an association request message preferably according to the IEEE 802.11i standard. Said association request message comprises an authentication suite
- 25 30 35 40 45 50 55 element indicating IEEE 802.1x authentication. The access point further comprises sending means for sending the identifier data of the authenticated terminal to the list of the access controller if the terminal device is using

the authentication method wherein the access point relays authentication information between the terminal and the authentication server. The access point further comprises relaying means 206 for relaying authentication information between the terminal device and one of the following: the authentication server if the terminal device is using the first authentication method, the authentication agent if the terminal device is using the second authentication method. In cases when the logical access control functionality is contained in the access point, the access point further comprises access control means 208 for relaying data packets of authenticated terminals and blocking data packets of unauthenticated terminals.

[0025] A terminal employing the open system authentication method receives an IP address for use from the DHCP server, which may be located at the authentication agent or, alternatively, at the access point or elsewhere in the network. The access point 200 relays authentication messages between the terminal and the authentication agent, which operates as the authenticator entity and authenticates the terminal device by using the IP-based authentication method of the third protocol layer. The authentication agent typically uses the authentication service provided by the authentication server by further relaying the authentication information between the terminal device and the authentication server, which verifies the authentication information. After the authentication, the authentication agent sends information about a successful authentication and the identifier data of the terminal, such as the terminal IP address or MAC address, to the access controller, which adds it to the access control list and starts to relay the data packets of the terminal.

[0026] When a terminal uses the IEEE 802.1x protocol for authentication, the access point operates as the authenticator entity and authenticates the terminal by using the IEEE 802.1x protocol of the second protocol layer. The access point typically uses the authentication service provided by the authentication server by relaying the authentication information between the terminal device and the authentication server, which verifies the authentication information. The access point sends information about a successful authentication and the identifier data of the terminal, such as the terminal IP address or MAC address, to the access controller, which adds the identifier data of the terminal to the access control list and starts to relay the data packets of the terminal.

[0027] Figure 3 shows the present Nokia Operator WLAN system. The system comprises a wireless terminal device 303, such as a WLAN terminal, being configured to use the open system authentication in order to authenticate itself to the network, an access point 301, for providing a wireless connection from the communications device 303 to the network, an access controller 302 for relaying authentication information between the terminal device 303 and an authentication server 307,

for maintaining an access controller list 309 of authenticated terminal devices (e.g. terminal device 303) and for relaying data packets of said authenticated terminal devices included on the list 309. The system further

- 5 5 comprises the authentication server 307 for providing an authentication service to an authenticator, such as the access point 301 by determining whether the terminal device is authorized to access the services provided by the access point. The system may further comprise servers, such as a DHCP server 305 for providing an IP-address to the terminal device 302 when using the open system authentication, an accounting server 306 for accounting the amount of data transferred to and from the terminal device and a router for routing data packets of the terminal device.

[0028] When authentication of the wireless terminal device according to the third protocol layer, such as the open system authentication, is carried out, the terminal device 303 associates with the access point 301. Authentication is not carried out at this point yet. An IP address is formed for the terminal device 303 by means of the DHCP protocol, for example. Then follows the actual third protocol layer authentication. In an embodiment of the WLAN system, for example, the communications device 303 broadcasts a paging message to page an authentication server 307, the message being answered by the authentication server 307. On the basis of the reply message, the terminal device 303 knows that the network in question requires IP-based, third protocol layer authentication between the terminal device 303 and the access controller 302. The access controller 302 exchanges authentication messages with the authentication server 307. In SIM authentication, for example, the International Mobile Subscriber Identity (IMSI) is transmitted to the authentication server 307. The access controller 302 communicates with the authentication server 306 by using an AAA protocol (Authentication, Authorization, Accounting), such as the RADIUS (Remote Authentication Dial In User Service) or the DI-

- 20 25 AMETER protocol.
- 30 35 **[0029]** The authentication server 307 obtains GSM challenges (GSM challenge is a parameter, i.e. 128 bit random number, used in a GSM authentication), and sends the challenges to the access controller 302, using the AAA protocol, which further relays them to the terminal device 303 using the third protocol layer authentication protocol NAAP. The terminal device 303 then calculates a response value corresponding to the issued challenge by using a secret key stored in the SIM card.

- 40 45 **[0029]** The authentication server 307 obtains GSM challenges (GSM challenge is a parameter, i.e. 128 bit random number, used in a GSM authentication), and sends the challenges to the access controller 302, using the AAA protocol, which further relays them to the terminal device 303 using the third protocol layer authentication protocol NAAP. The terminal device 303 then calculates a response value corresponding to the issued challenge by using a secret key stored in the SIM card.
- 50 55 The response value is a 32 bit number and the terminal device sends the response to the access controller 302, with the third protocol layer authentication protocol. The access controller 302 relays the information to the authentication server 307 with the AAA protocol. The authentication server 307 verifies the response by checking whether the terminal has calculated a correct response value or not. If the received response is correct, the authentication server 307 sends an indication of suc-

cessful authentication to the access controller 302 with the AAA protocol, which relays the indication to the terminal 303 with the third protocol layer authentication protocol. After the authentication, the identifier data of the terminal device 303 is added to the access control list 309 by the access controller 302. The access controller 302 only transmits data packets of the communications device whose identifier data, such as an IP or MAC address, is found on the list 309.

[0030] Figure 4 shows a system according to the IEEE 802.1x protocol. The system comprises a wireless terminal device 404, such as a WLAN terminal, configured to use the authentication method according to IEEE 802.1x protocol in order to authenticate itself to the network, an access point 401 for setting up a communication connection to the terminal device 404 and for relaying authentication information between the terminal device 404 and an authentication server 402. The system further comprising the authentication server 402 for providing an authentication service to an authenticator, such as the access point 401 by determining whether the terminal device 404 is authorized to access the services provided by the access point 401 and an accounting server 405 for accounting the amount of data transferred to and from the terminal device. The system further comprising one or more routers 403 for routing data packets of the terminal device 404.

[0031] The authenticator entity, such as the access point 401, typically communicates with the authentication server 402 by using an AAA protocol (Authentication, Authorization, Accounting), similarly to the Nokia Operator Wireless LAN solution described above in Figure 3. When the terminal is successfully authenticated the access point relays data packets between the terminal device 404 and the router 403.

[0032] Figure 5 shows a system according to an embodiment of the invention. In the following the invention is exemplary illustrated in an environment that comprises a wireless terminal device 303, such as a WLAN terminal, that can authenticate by using third protocol layer authentication method, such as open system authentication and a wireless terminal device 404, such as a WLAN terminal, that can authenticate by using the authentication method according to the IEEE 802.1x standard, such as a Wireless LAN terminal that uses the IEEE 802.11i standard. The terminals are capable of setting up a connection to a communications network, which comprises an access point 501, for providing a wireless connection from the communications device 303, 304 to the network and for relaying authentication information between the terminal device 404 and an authentication server 505. The access point comprises a logical access controller functionality 502 for relaying data packets of the authenticated terminal and blocking data packets of unauthenticated terminals, and a list 503 of authenticated terminal devices. The access controller functionality 502 and the list 503 may alternatively be located for example in an authenticating agent 504, rout-

er 508 or somewhere else in the network. The system further comprises an authentication agent 504 for relaying authentication information between the terminal device 303 and the authentication server 505. The system

- 5 further comprises servers, such as a DHCP server 506 for providing an IP-address for the terminal device 303, an accounting server 507 for accounting the amount of data transferred to and from the terminal device, and an authentication server 505 for providing an authentication service to an authenticator. The authenticator is one of the following: the access point 501 and the authentication agent 504. The authentication server 505 determines whether the terminal device is authorized to access the services provided by the authenticator. The
- 10 system also comprises one or more routers 508 for routing data packets of the terminal devices 303, 404.
- 15

[0033] The access point 501 sends messages, such as beacon messages according to IEEE 802.11i or IEEE 802.11 standard, to the surrounding of the access point.

- 20 Said beacon message may comprise authentication suite element that further comprises information of the authentication method the access point can handle, e.g. the authentication method according to the IEEE 802.11i standard. A wireless terminal 404 that implements the IEEE 802.11i standard will recognise that the access point supports the IEEE 802.1x authentication protocol. A wireless terminal 303 that does not implement the IEEE 802.11i standard does not process the authentication suite element, but it interprets the beacon message according to the IEEE 802.11 standard and hereby recognises that the access point 501 supports open system associations. The terminal 303, 304 receives the beacon message sent from the access point 501. The terminal device 303, 404 may get several beacon messages from several access points that are inside the range of the terminal. Alternatively to beacon messages, the terminal 303, 404 can also learn of local access points by sending messages, such as probe request message according to the IEEE 802.11i standard
- 25 or the IEEE 802.11 standard, to all access points inside the range of the terminal. When the access point 501 receives the probe request message the terminal 303, 404 sends, in response to said probe request, a message, such as probe response message according to
- 30 IEEE 802.11i or IEEE 802.11 standard. The probe response message to the terminal device 404 is sent according to the IEEE 802.11i standard and it comprises the authentication suite element that comprises information of the authentication method. The probe response message to the terminal device 303 may be sent according to the IEEE 802.11 standard and hence it does not need to include the authentication suite element. The terminal 303, 404 receives the probe response message from the access point 501. The terminal device 303, 404 may get several probe response messages from several access points that are inside the range of the terminal.
- 35
- 40
- 45
- 50
- 55

[0034] After discovering suitable local access points

based on beacon messages or probe messages, the terminal device 303, 404 selects the access point that supports the authentication method the terminal is using. The terminal device 404 that supports the IEEE 802.11i standard and wishes to use the IEEE 802.1x authentication method adds the authentication suite element to the message, such as an association request message according to IEEE802.11i standard. The terminal device 303 that wishes to use open system authentication first starts the open authentication by sending an authentication request message, to which the access point 501 replies with an authentication response message indicating success. The open authentication is followed by association. The terminal device 303 does not include an authentication suite element in the association messages it sends. After that the terminal 303, 404 sends the association request message to the access point. On the basis of the authentication or association request message the access point 501 identifies the authentication method the terminal device 303, 404 is using.

[0035] When authentication of the wireless communication device according to the third protocol layer is carried out, the communications device 303 associates with the access point 501, authentication being not carried out at this point yet. An IP address is formed for the communications device 303 by means of the DHCP protocol, for example. Then follows the actual third protocol layer authentication. In an embodiment of the WLAN system, for example, the terminal device 303 broadcasts a paging message to page an authentication agent 504, the message being answered by the authentication agent. On the basis of the reply message, the communications device 303 knows that the network in question requires IP-based, third protocol layer authentication between the communications device 303 and the authentication agent 504. The authentication agent 504 exchanges authentication messages with the authentication server 505 using an AAA protocol. The authentication procedure is similar to the Nokia Operator Wireless LAN system described in Figure 3. The authentication agent 504 receives a notification of successful authentication from the authentication server 507 by means of the AAA protocol. After the authentication, the authentication agent sends the identifier data, such as an IP-address, of the terminal device 303, to the access controller functionality 502. In this embodiment, the access controller functionality 502 is implemented in the access point device 501. The authentication agent 504 sends a message to the access point 501. For example, the message can be formed using the User Datagram Protocol (UDP) over the Internet Protocol (IP). The message includes at least the identifier data of the terminal device 303. Upon receipt of the message, the access controller functionality 502 in the access point 501 adds the identifier data to the access control list 503. The access controller functionality 502 only relays data packets of the terminal device whose

identifier data, such as an IP or MAC address, are found on the list 503. Authentication must typically be repeated after a specific period of time by the communications device, for example if the terminal device is switched off

- 5 (due to low battery level), leaves the network (shadow region) or automatically discontinues the use of a service. The access controller 502 keeps a record of the duration of the connection of the communications device 303 and the number of data packets transmitted/received.
- 10 The access controller 502 sends the information to the authentication server 505 or the accounting server 507, for example, to serve as a basis for user billing. Alternatively, authentication according to the third protocol layer can be carried out such that when the user
- 15 activates a World Wide Web (WWW) browser, the authentication agent 504 sends to the browser of the terminal 303 a page inquiring about the user identification and the password, whereby the user is identified and added to the access control list 503. Yet alternatively,
- 20 authentication according to the third protocol layer can be carried out using a Virtual Private Network (VPN) software, in which the user authentication is typically performed as part of the Internet Key Exchange (IKE) protocol.
- 25 **[0036]** In the second protocol layer authentication, the communications device 404 and the access point 501 agree already during the association that they will be using WLAN authentication (and not open system authentication as in the third protocol layer authentication).
- 30 The WLAN authentication is carried out as specified in the IEEE 802.1x protocol. After a successful authentication, the access controller functionality 502 is informed of the event and it adds the terminal device 304 authenticated according to the second protocol layer to
- 35 the access control list 503 and starts to relay the packets of the authenticated terminal device. Because the access controller functionality 502 is implemented in the access point device 501, the access point 501 is capable of locally sending the identifier data of the terminal to the access controller functionality 502. The access control list 503 comprises identifier data of terminals authenticated according to both the third and the second protocol layer. After the second protocol layer authentication, the authentication agent 504 does not need to
- 40 subject the terminal device 404 to third protocol layer authentication any more, because the identifier data of the terminal device 404 are already in the list 503.
- 45 **[0037]** In an alternative embodiment of this invention, service differentiation is provided for different classes of
- 50 terminal devices. Figure 6 shows a flow diagram of a method according to the alternative embodiment of the invention. In step 601 an access point, and a terminal device, such as a wireless communications device, set up a connection and associate with each other. On the
- 55 initiative of the access point, the routine then checks whether authentication according to the second protocol layer or open system authentication according to the third protocol layer is concerned. The terminal establish-

es communications with the access point by sending an authentication or an association request to the access point. The request comprises a request to authenticate by using the authentication method the device is using. In step 602 WLAN access point classifies WLAN clients to different classes preferably based on the authentication method used by the WLAN clients or based on some other parameters that are exchanged during association and authentication phase. In step 603 the access point relays data packets on the basis of the classification. The client class is taken into account when relaying data packets between the wireless network and the wired network (Distribution System, DS). For example, the authentication method, which is selected on association, may be used to classify users so that open system clients are directed to a different Virtual LAN (VLAN) than IEEE 802.1x/802.11i clients. In the 802.1x case, the access point may further differentiate clients based on the realm name portion of the user identity (Network Access Identifier, NAI). The realm name identifies the RADIUS server that authenticates the user. For example, a corporate WLAN access point may direct clients that are authenticated by the corporate RADIUS server to a different VLAN than clients that are authenticated by other RADIUS servers. For the sake of simplicity, the authentication method (open system or IEEE 802.1x) is used here as an example of the parameter by which the access point classifies wireless terminals into different classes. A person skilled in the art will find it apparent that the invention is not restricted to terminal classification by authentication method and that there are other parameters by which the access point may divide terminals into separate classes. The access point can use any parameter it learns upon communications establishment as a basis of classification. The parameter may be related to the radio technology, authentication or association or other areas of communication establishment, such as the radio frequency band, data rate used by the terminal, the Network Access Identifier or a part of it, or the Extensible Authentication Protocol (EAP) type used in IEEE 802.1x authentication.

[0038] Figure 7 shows an access point according to an alternative embodiment of the invention. The access point 700 comprises a processor 701 and memory 702 for executing the operations in question and at least one application 703 for carrying out e.g. identifying of an authentication method. The access point 700 further comprises an interface 705 for connecting to the router, to servers, such as an access controller, or authentication server, for example. The access point further comprises identifying means 707 for identifying, upon communication establishment, whether the terminal device is using the first or the second authentication method. Preferably the access point identifies the authentication method by receiving a message from the terminal, said message comprising the authentication method the terminal is using. If the terminal is using the first authentication method, the message is preferably association request mes-

sage according to IEEE 802.11i standard, said association request message comprising an authentication suite element indicating IEEE 802.1x authentication. If the terminal is using the second authentication method,

- 5 the message is preferably authentication request message according to IEEE 802.11 standard, said authentication request message indicating open system authentication. The device further comprises classifying means 704 for classifying terminals to different classes based on the identified authentication method. The access point further comprises relaying means 706 for relaying data packets of the wireless terminals between the wireless network and the wired network, said relaying means taking the client class into account by directing data packets of terminal devices of different classes to separate logical channels. The use of different Virtual LANs for different terminal classes is an example of how to take the terminal class into account when relaying data packets. Upon receipt of a data packet from a wireless terminal, the access point first detects the terminal class of the sending wireless terminal preferably based on the source MAC address field in the data packet and then relays the data packet to the wireless network using the Virtual LAN Identifier associated with the terminal class,
- 10 15 20 25 30 35 40 45 50 55
- so that packets from open system clients are relayed using a different Virtual LAN identifier than packets from 802.1x clients. Furthermore, upon receipt of a unicast data packet from the wired network, the access point first detects the terminal class of the destination wireless terminal, preferably based on the destination MAC address field in the data packet, and then verifies that the Virtual LAN Identifier in the data packet is correct, i.e. what it should be for the detected terminal class. The access point only relays the data packet to the destination wireless terminal if the packet was received from the wired network with the correct Virtual LAN Identifier. If the Virtual LAN identifier is incorrect, the access point preferably discards the data packet. Upon receipt of a multicast or broadcast data packet from the wired network, the access point cannot detect the terminal class of a single terminal device, because there may be several destinations. In this case, the access point may still process the data packets according to the terminal class indicated in the Virtual LAN identifier. For example multicast or broadcast data frames destined to open system clients may be transmitted without encryption or integrity protection, whereas IEEE 802.11 i packet security may be applied to multicast or broadcast data frames destined to IEEE 802.1x clients.
- [0039]** Alternatively to Virtual LANs, the access point may differentiate the data packets based on IP subnet-network or IP address range. In this example, the access point ensures that the wireless terminal is assigned an IP address from the IP subnetnetwork or range that corresponds to the terminal class identified upon communications establishment. Preferably, the access point relays the DHCP packets sent by the wireless terminal on IP configuration phase to a suitable DHCP server based

on terminal class, so that the terminal is assigned an address from the correct IP subnetwork or IP address range. Upon receipt of a data packet from a wireless terminal, the access point first detects the terminal class preferably based on the source MAC address field in the data packet and then verifies that the source IP address field (or another protocol field that comprises an IP address) in the received data packet belongs to the correct IP subnetwork or IP address range, associated with the detected terminal class. The access point only relays the data packet to the wired network if this verification succeeds. If this verification fails, the access point preferably discards the data packet. Further, upon receipt of a unicast data packet from the wired network, the access point first detects the terminal class preferably based on the destination MAC address field, and then verifies that the destination IP address field in the data packet belongs to the correct IP subnetwork or IP address range, associated with the detected terminal class. The access point only relays the data packet to the destination wireless terminal if this verification succeeds. If this verification fails, the access point preferably discards the data packet. Upon receipt of a multicast or broadcast data packet from the wired network, the access point still be able to detect a correct terminal class based on a protocol field comprising an IP address. Different processing, such as different encryption or integrity protection, may be applied to multicast or broadcast data packets destined to open system clients and IEEE 802.1x clients. For the sake of simplicity, use of separate Virtual LANs for different client classes is used as an example of how the access point takes the terminal class into account when relaying data packets between the wireless terminals and the wired network. A person skilled in the art will find it apparent that the invention is not restricted to the use of different Virtual LANs for each terminal class and that there are other ways of taking the terminal class into account in relaying data packets. Alternatively to Virtual LANs, the access point may take the terminal class into account by using any method of differentiating data packets into separate logical channels, based on terminal class, when relaying data packets between the wireless network and wired network. Another example of said method is packet tunnelling to different destinations based on terminal class. Upon receipt of a data packet from the wireless terminal, the access point detects the terminal class preferably based on the source MAC address field in the received packet. The access point then encapsulates the received packet within a new packet. The destination of the new packet is chosen based on the terminal class, so that different terminal classes are tunnelled to different destinations. The encapsulation is preferably IP encapsulation, wherein the original MAC header is removed, and the resulting IP packet is encapsulated within a new IP packet. The IP packet is then forwarded according to the new IP destination address. Correspondingly, the data packets received from the wired network

may also be tunnelled. Upon receipt of a data packet from the wireless network, the access point detects the terminal class preferably based on the source IP address in the outer IP header, when different tunnel starting points are used for each terminal class. The access point then decapsulates the tunnelled packet and relays the resulting data packet to the destination wireless terminal.

5 [0040] Figure 8 shows a system according to an alternative embodiment of the invention. In the following 10 the invention is exemplary illustrated in an environment that comprises a terminal device 303 that can authenticate by using third protocol layer authentication method, such as open system authentication and a terminal 404 15 that can authenticate by using the authentication method according to the IEEE 802.1x standard, such as a Wireless LAN terminal that uses the IEEE 802.11i standard. The terminals are capable of setting up a connection to a communications network, which comprises an 20 access point 801, for providing a wireless connection from the communications device 303, 304 to the network and for relaying authentication information between the terminal device 404 and an authentication server 806. The system further comprising access controller 802, that comprises a logical access controller functionality for relaying data packets of the open system authenticated terminal and blocking data packets of unauthenticated terminals, and a list 803 of authenticated open system terminal devices. The access controller 802 is relaying authentication information between the terminal device 303 and the authentication server 805. The system further comprises servers, such as a DHCP server 804 for providing an IP-address for the terminal device 303, accounting server 805 for accounting 30 the amount of data transferred to and from the terminal device, and authentication server 806 for providing an authentication service to an authenticator, said authenticator being one of the following: the access point 801 and the access controller 802, by determining 35 whether the terminal device is authorized to access the services provided by the authenticator, and one or more routers 807 for routing data packets of the terminal devices 303, 404.

40 [0041] This example system is arranged such that 45 network access control for the open system terminal 303 is implemented in the access controller device 802, and network access control for the IEEE 802.1x terminal 404 is implemented in the access point device 801. The arrangement is based on data packet classification, in the 50 access point device 801, into separate logical channels based on terminal authentication method.

[0042] When a terminal device 303 that uses the open system authentication method establishes communications with the access point, the access point 801 assigns 55 the terminal 303 to a terminal class for which the access controller 802 employs access control at the third protocol layer. By use of Virtual LANs, the access controller 802 is configured to enforce access control to data pack-

ets received with a Virtual LAN Identifier assigned to open system terminals. If separate IP sub networks or IP address ranges are used to separate data packets into logical channels, the access controller 802 is configured to enforce access control to data packets of terminals 303 that use an IP address from the IP sub network or address range of open system terminals.

[0043] When a terminal device 404 establishes communications with the access point 801 and authenticates with the IEEE 802.1x authentication method, the access point 801 assigns the terminal 404 to a terminal class for which the access controller 802 does not employ access control. With Virtual LANs, it is possible to configure the access controller 802 to route data packets with the Virtual LAN identifier associated with the IEEE 802.1x terminal 404 without enforcing any access control. Alternatively, the Virtual LAN associated with the IEEE 802.1x terminals 404 may employ another router device 807 through which the data packets of IEEE 802.1x terminals 404 are routed, so that the data packets do not traverse the access controller 802. If separate IP sub networks or IP address ranges are used to separate data packets into logical channels, the access controller 802 may be configured to route data packets of terminals 404 that use an IP address from the IP sub-network or address range of IEEE 802.1x terminals without enforcing access control.

[0044] The alternative embodiment of the invention according to figures 6 to 8 makes it possible to use the same WLAN radio network for several purposes. The same radio network can serve legacy WLAN clients, such as OWLan release 1 clients that use open system authentication, and new WLAN clients that use the new IEEE standards, such as OWLan release 2 clients that use IEEE 802.1x authentication. An extreme access point implementation of this invention could look like two separate access points to the wireless clients. One of the "virtual" access points would allow open system associations and the other access point 802.1x associations. A simpler implementation would look like a single access point but it would support both open association and 802.1x association.

[0045] Another object for the alternative embodiment are protected networks that are currently built on Virtual Private Network (VPN) technology, such as corporate networks. An access point that implements this invention would be able to route open system clients to the existing LAN which is separated with a VPN gateway from the protected network. Open system clients will therefore need to establish a VPN connection in order to access the protected network. The access point could route IEEE 802.11i clients to a different Virtual LAN, which has direct connectivity to the protected network. Hence, this invention provides a managed deployment path from the current corporate WLAN solution to the new IEEE 802.11i solution.

[0046] In another example system employing the alternative embodiment of this invention, the terminal

classification in the access point device can be used to direct data packets of terminal devices that use open system authentication to an uncontrolled network, on which no access control is enforced. Said uncontrolled

5 network may be a local Intranet or other network with limited and free resources that are available to anyone. In this example, the data packets of terminal devices that use IEEE 802.1x authentication are directed to a controlled network, such as the global Internet. Said controlled network is such that it is only available to terminals that authenticate using the IEEE 802.1x authentication method.

[0047] Advantages of the alternative embodiment described above are: a single WLAN radio network is able 15 to securely support both legacy and new WLAN clients, legacy and new WLAN clients may use different IP sub networks and different services, no support required in wireless stations.

[0048] The invention is not restricted to open system 20 authentication and authentication according to IEEE802.11i protocol or the IEEE 802.1x protocol. The first embodiment of the invention can be used in any such system wherein a terminal can access to network by using an access point or authentication agent as an authenticator. The second embodiment of the invention can be used in any such system wherein it is advantageous to provide different service to different terminal classes, said terminal class identified based on a parameter of the communication establishment.

[0049] The above disclosure illustrates the implementation 25 of the invention and its embodiments by means of examples. A person skilled in the art will find it apparent that the invention is not restricted to the details of the above-described embodiments and that there are 35 also other ways of implementing the invention without deviating from the characteristics of the invention. The above embodiments should thus be considered as illustrative and not restrictive. Hence the possibilities of implementing and using the invention are only restricted 40 by the accompanying claims and therefore the different alternative implementations of the invention, including equivalent implementations, defined in the claims also belong to the scope of the invention.

45

Claims

1. A method for relaying data packets of a wireless terminal device in a communication network, the network comprising;

50
55 an access point for setting up a communication connection to the terminal device,
an access controller for relaying authentication information between the terminal device and an authentication server,
an authentication server for providing an authenticating service for the terminal device to

authenticate to the network,
the terminal device being configured to use one
of the following authentication methods in order
to authenticate itself to the network: a first authen-
tication method wherein the access point
relays authentication information between the
terminal device and the authentication server,
a second authentication method wherein the
access controller relays authentication informa-
tion between the terminal device and the authen-
tication server,
the method comprising establishing a commu-
nication connection between the terminal de-
vice and the access point,

characterized by the method further com-
prising the steps of

identifying at the access point a parameter re-
lating to the step of establishing the communica-
tion connection,
classifying the terminal device on the basis of
the identified parameter and
directing data packets of terminal devices of dif-
ferent classes to separate logical channels.

- 2. A method according to claim 1, **characterized in**
that the identified parameter is the authentication
method used by the terminal.
- 3. A method according to claim 2, **characterized in**
that the authentication method is one of the follow-
ing: an open system authentication and an authen-
tication according to 802.1x protocol.
- 4. A method according to claim 1, **characterized in**
that the identified parameter is one of the following:
the Network Access Identifier, part of the Network
Access Identifier used by the terminal device, fre-
quency band, data rate, used radio technology of
the terminal device, .
- 5. A method according to claim 1, **characterized in**
that the separate logical channels are one of the
following: Virtual LANs, IP sub networks and IP ad-
dress ranges.
- 6. A method according to claim 5, **characterized in**
that the access point ensures that the terminal de-
vice is assigned an IP address from the correct IP
sub network or IP address range.
- 7. A method according to claim 1, **characterized in**
that the separate logical channels are tunnels.
- 8. A method according to claim 1, **characterized in**
that the access point verifies for data packets that,
the logical channel used, matches the identified ter-

minal device class.

- 9. A method according to claim 8, **characterized in**
that the access point only relays data packets for
which said verification is successful and discards
data packets for which said verification is unsuc-
cessful.
- 10. A method according to claim 1, **characterized in**
that the access point applies different security
processing to data packets of different terminal de-
vice classes.
- 11. An access point (700) for setting up a communica-
tion connection to a terminal device in a network,
said network comprising:

an access controller for relaying authentication
information between the terminal device and an
authentication server,
an authentication server for providing an au-
thenticating service for the terminal device to
authenticate to the network,
said access point comprising
establishing means (701-703, 705) for estab-
lishing a communication connection between
the terminal device and the access point,

characterized in that the access point is config-
ured to accept the terminal device to use one of the
following authentication methods in order to au-
thenticate itself to the network: a first authen-
tication method wherein the access point is configured to
relay authentication information between the termi-
nal device and the authentication server, a second
authentication method wherein the access point is
configured to relay authentication information be-
tween the terminal device and an authentication
agent, whereby the access point further comprises

identifying means (707) for identifying a par-
meter relating to the establishment of the com-
munication connection,
classifying means (704) for classifying the ter-
minal device on the basis of the identified pa-
rameter and
directing means (701-703, 705, 706) for direct-
ing data packets of terminal devices of different
classes to separate logical channels.

- 12. An access point according to claim 11, **character-
ized in that** said identifying means are arranged to
identify the parameter in response to detecting one
of the following: authentication method used by the
terminal device, the Network Access Identifier or
part of the Network Access Identifier used by the
terminal device, frequency band, data rate and
used radio technology of the terminal device.

13. An access point according to claim 11, **characterized in that** said directing means are arranged to use one of the following as said separate logical channels: Virtual LANs, IP sub networks and IP address ranges.

5

14. An access point according to claim 11, **characterized in that** the access point further comprising verifying means for verifying data packets that, the logical channel used, matches the identified terminal device class.

10

15. An access point according to claim 11, **characterized in that** the access point is arranged to only relay data packets for which said verification is successful and discards data packets for which said verification is unsuccessful.

15

16. A method for access control of a wireless terminal device in a communication network, the network comprising

20

an access point for setting up a communication connection to the terminal device,
 an authentication agent for relaying authentication information between the terminal device and an authentication server,
 a logical access controller functionality for relaying data packets of the authenticated terminal device and blocking data packets of unauthenticated terminal devices, the logical access controller functionality further comprising a list of authenticated terminal devices,
 an authenticating server for providing an authenticating service for the terminal device to authenticate to the network,
 the terminal device being configured to use either of the following authentication methods in order to authenticate itself to the network: a first authentication method wherein the access point relays authentication information between the terminal device and the authentication server, a second authentication method wherein the authentication agent relays authentication information between the terminal device and the authentication server, **characterized by** the method comprising the steps of

25

identifying at the access point whether the terminal device is using the first or the second authentication method,
 whereby if the terminal device authenticates by using the first authentication method, performing the steps of:

30

the access point relaying authentication information between the terminal device and the authentication server,

the access point sending the identifier data of the terminal device, in response to successful authentication, to the list of the access controller functionality,

the access controller functionality adding the identifier data of the authenticated terminal device to the list and relaying data packets of the terminal device included on the list and if the terminal device authenticates by using the second authentication method, performing the steps of:

the access point relaying authentication information between the terminal device and the authenticating agent, the authentication agent relaying authentication information between the terminal device and the authentication server,
 the authentication agent sending the identifier data of the terminal device, in response to successful authentication, to the list of the access controller functionality, and

the access controller functionality adding the identifier data of the authenticated terminal device to the list and relaying data packets of the terminal device included on the list.

17. A method according to claim 16, **characterized in that** the access controller functionality is implemented as part of the access point device.

35

18. A method according to claim 16, **characterized in that** the access controller functionality is implemented as part of the authentication agent device.

40

19. A method according to claim 16, **characterized in that** the access controller functionality is implemented in a device separate from the access point and the authentication agent.

45

20. A method according to claim 16, **characterized in that** the identifier data comprises at least one of the following: the IP address and the MAC address of the terminal device.

50

21. A method according to claim 16, **characterized in that** the first authentication method is performed according to IEEE 802.1X protocol.

55

22. A method according to claim 21, **characterized in that** the first authentication method is performed according to IEEE 802.11i protocol.

23. A method according to claim 16, **characterized in**

that the second authentication method is performed over the Internet protocol.

24. A method according to claim 23, **characterized in that** the second authentication method is performed according to one of the following: the internet key exchange protocol and the hypertext transfer protocol. 5

25. A method according to claims 21 to 24, **characterized in that** the access point identifies the authentication method by receiving an association request message from the terminal device. 10

26. A method according to claim 25, **characterized in that** the association request message comprising an authentication suite element, said authentication suite element further comprising the information of the authentication method the device is using. 15

27. A method according to any one of claims 17 to 26, **characterized in that** the method further comprises renewing the authentication after a time period. 20

28. An access point (200) for setting up a communication connection to a terminal device in a network, said network comprising

an authentication agent for relaying authentication information between the terminal device and an authentication server,
a logical access controller functionality for relaying data packets of authenticated terminal devices included on a list and blocking data packets of unauthenticated terminal devices,
an authenticating server for providing an authenticating service for the terminal device to authenticate to the network, **characterized in that** the access point is configured to accept the terminal device to use one of the following authentication methods in order to authenticate itself to the network: a first authentication method wherein the access point is configured to relay authentication information between the terminal device and the authentication server, a second authentication method wherein the access point is configured to relay authentication information between the terminal device and an authentication agent, whereby the access point comprises 30

identifying means (207) for identifying whether the terminal device is using the first or the second authentication method, first relaying means (201, 205, 206) for relaying authentication information between the terminal device and the authentication server if the terminal device was identified 35

to be using the first authentication method, first sending means (201, 205) for sending identifier data of the terminal device, in response to successful authentication of the terminal device according to the first authentication method, to the list of the access controller functionality,
second relaying (201, 205, 206) means for relaying authentication information between the terminal device and the authentication agent if the terminal device was identified to be using the second authentication method and
second sending means (201, 205) for sending identifier data of the terminal device, in response to successful authentication of the terminal device according to the second authentication method, to the list of the access controller functionality.. 40

29. An access point according to claim 28, **characterized in that** the identifying means are arranged to identify the authentication method by receiving an association request message from the terminal device. 45

30. An access point according to claim 29 **characterized in that** the identifying means are arranged to detect an authentication suite element from the association request message, said authentication suite element the information of the authentication method the device is using. 50

31. An access point according to claim 28 **characterized in that** the detecting means are arranged to detect successful authentication of the terminal device using said first authentication method by receiving a message from the authentication server. 55

32. An access point according to claim 28, **characterized in that** the detecting means are arranged to detect successful authentication of the terminal device using said second authentication method by receiving a message from one of the following: the authentication agent or the authentication server. 55

33. A system for access control of a wireless terminal device (303, 304) in a communication network, the network comprising:

an access point (501) for setting up a communication connection to the terminal device,
an authentication agent (504) for relaying authentication information between the terminal device (303) and an authentication server (505),
a logical access controller functionality (502) for relaying data packets of the authenticated 55

terminal device and blocking data packets of unauthenticated terminal devices, the logical access controller functionality further comprising a list (503) of authenticated terminal devices,
 5
 an authenticating server (505) for providing an authenticating service for the terminal device (303, 404) to authenticate to the network,
 the terminal device (303, 304) being configured to use one of the following authentication methods in order to authenticate itself to the network: a first authentication method wherein the access point (501) relays authentication information between the terminal device (404) and the authentication server (505), a second authentication method wherein the authentication agent (504) relays authentication information between the terminal device (303) and the authentication server (505), **characterized in**
that the system comprises:
 10
 15
 20

identifying means for identifying at the access point (501) whether the terminal device (303, 404) is using the first or the second authentication method,
 25
 first relaying means for relaying at the access point (501) the authentication information of the first authentication method between the terminal device (404) and the authentication server (505),
 30
 second relaying means for relaying information between the terminal device (303) and the authentication agent (504),
 third relaying means at the authentication agent (504) for relaying authentication information of the second authentication method between the access point (501) and the authentication server (505),
 35
 first sending means for sending from the access point (501) identifier data of the terminal device (404), in response to successful authentication of the terminal device according to the first authentication method, to the list (503) of the access controller functionality (502),
 40
 45
 second sending means for sending from the authentication agent (504) the identifier data of the terminal device (303), in response to successful authentication of the terminal device according to the second authentication method, to the list (503) of the access controller functionality (502) and
 50
 relaying means at the access controller functionality (502) for relaying data packets of the terminal device (303, 404) included on the list.
 55

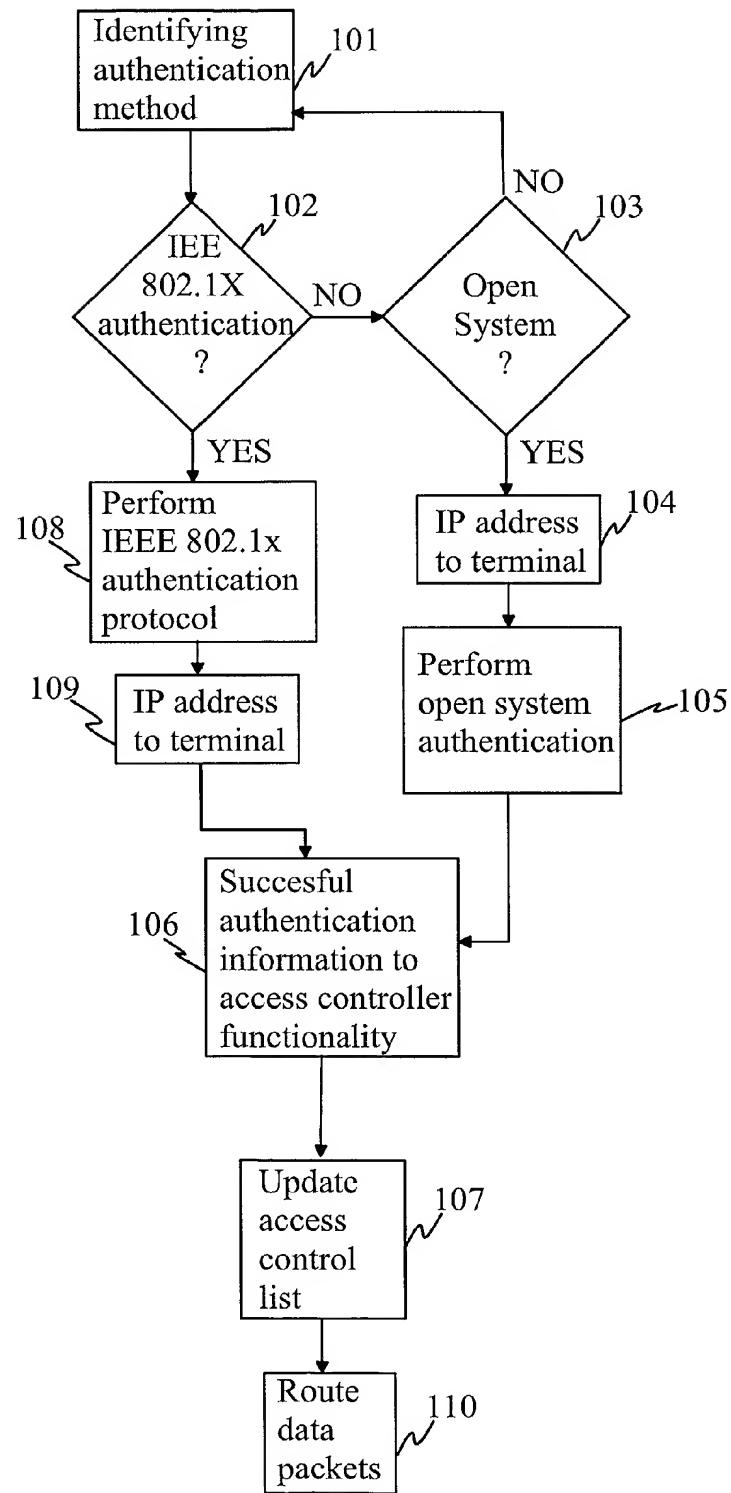


Fig. 1

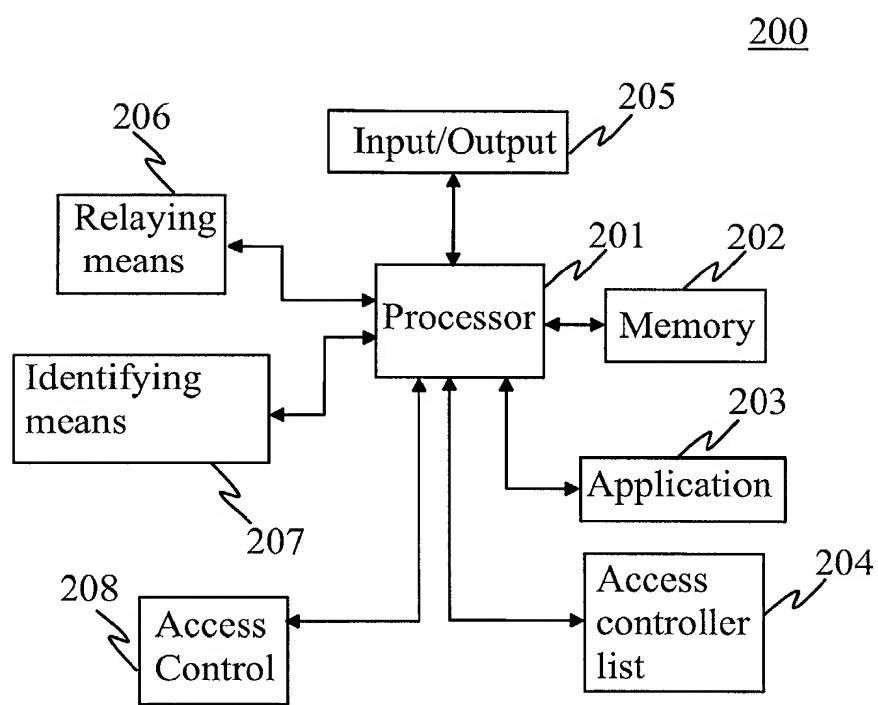
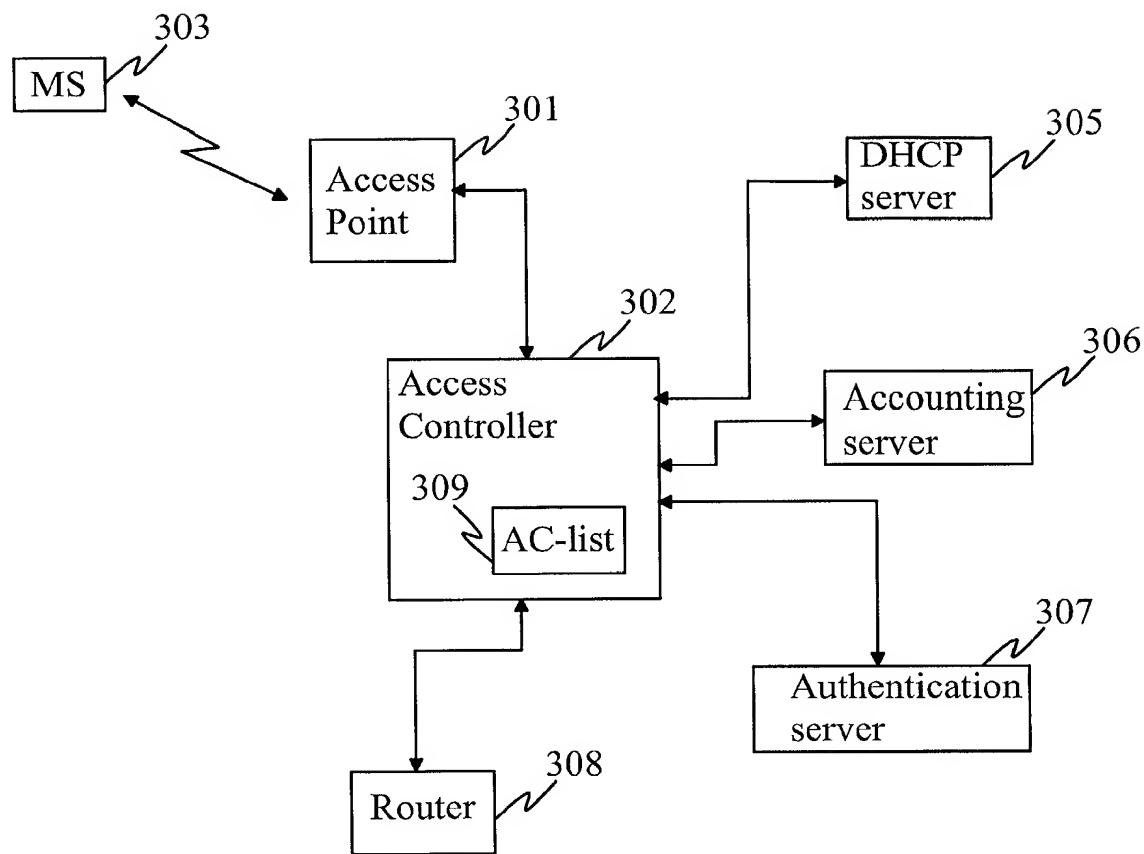


Fig. 2



Prior Art

Fig. 3

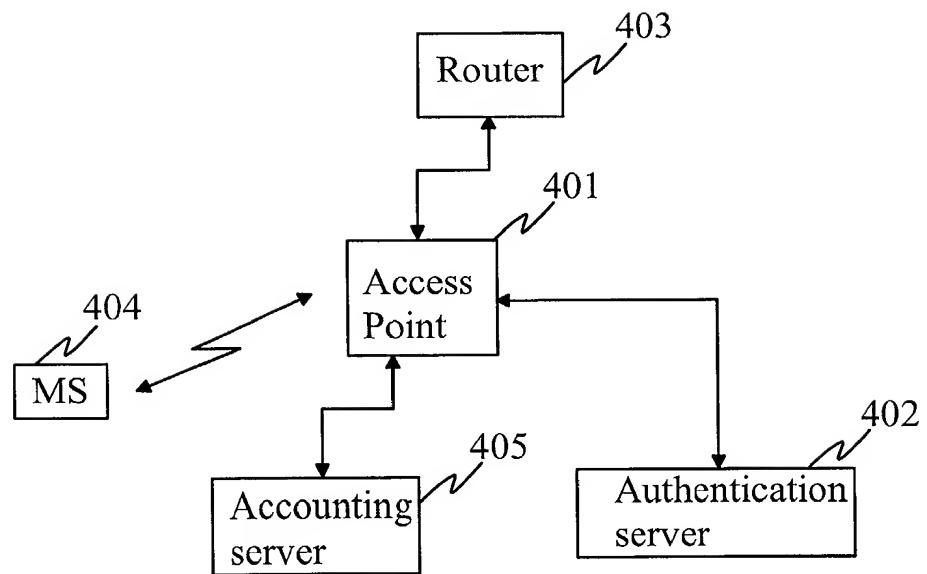


Fig. 4

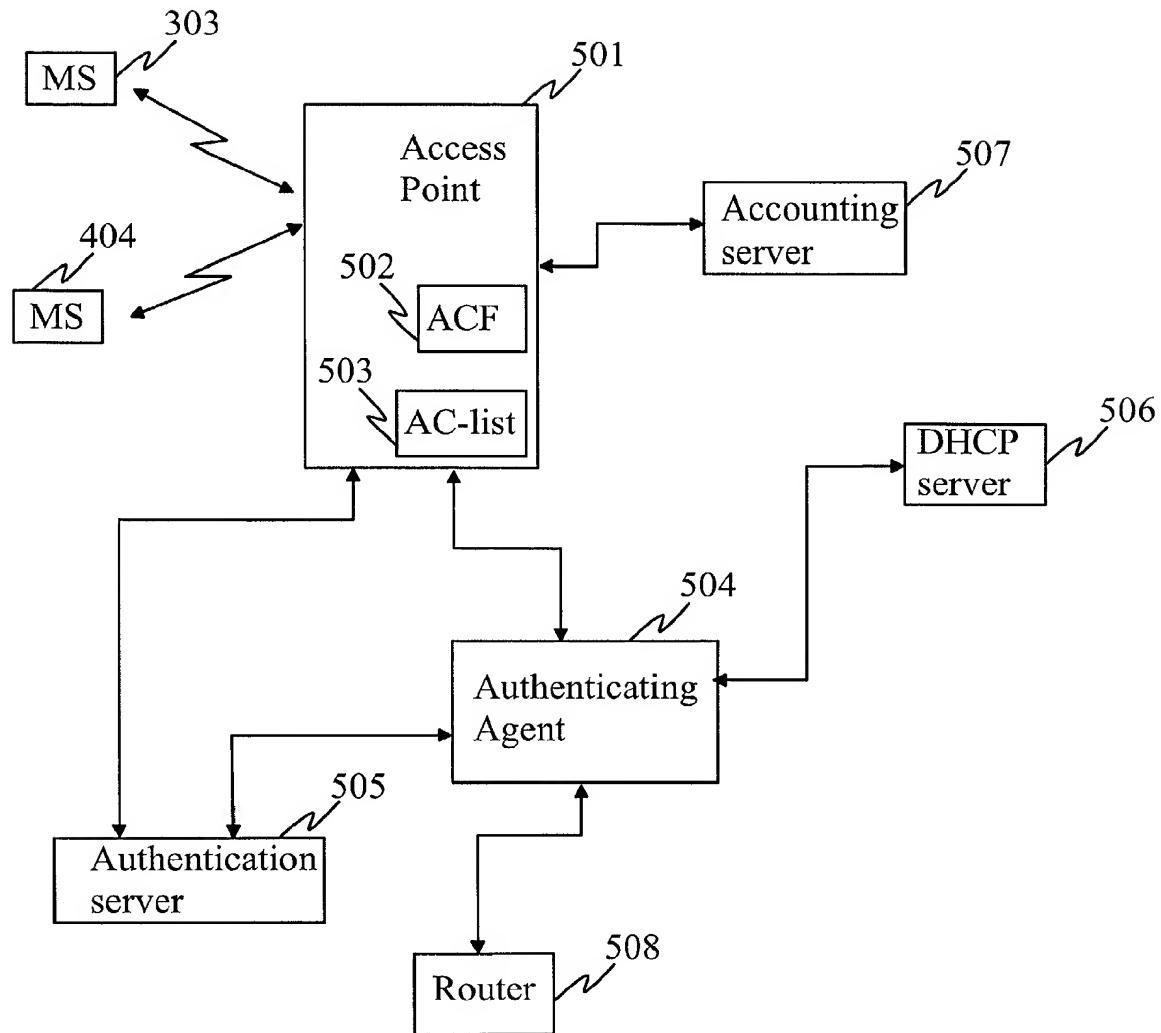


Fig. 5

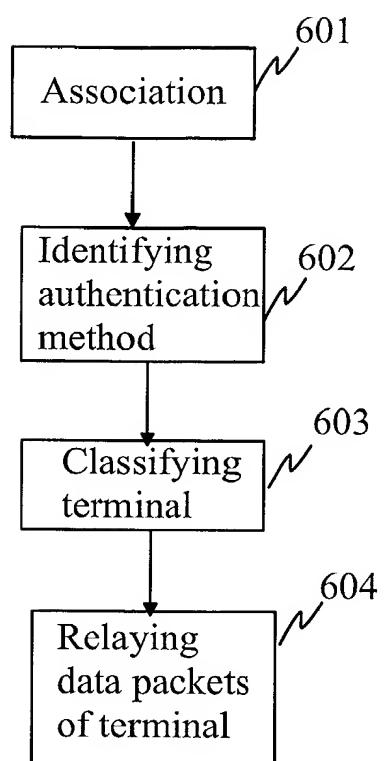


Fig. 6

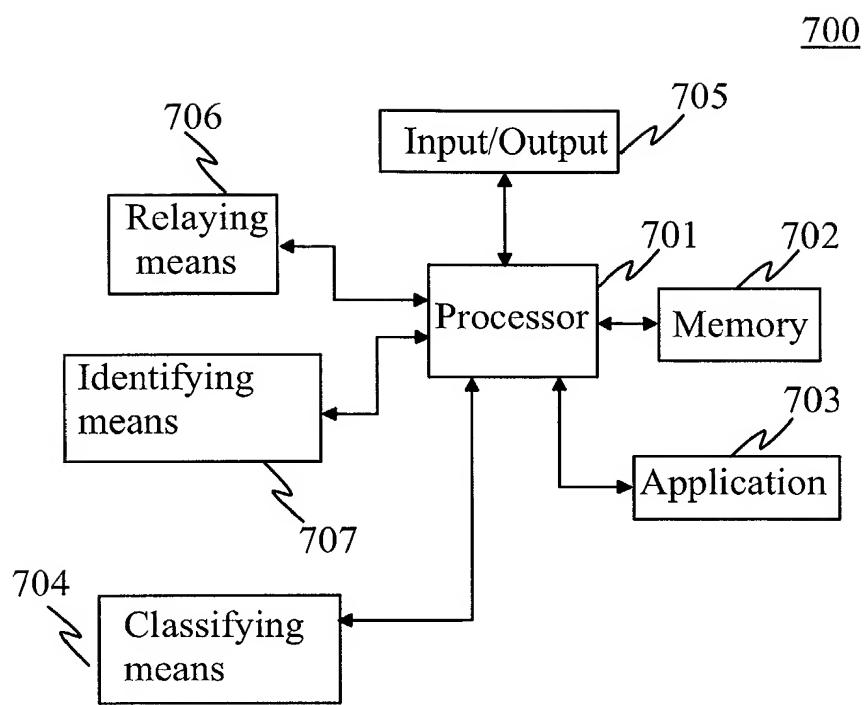


Fig. 7

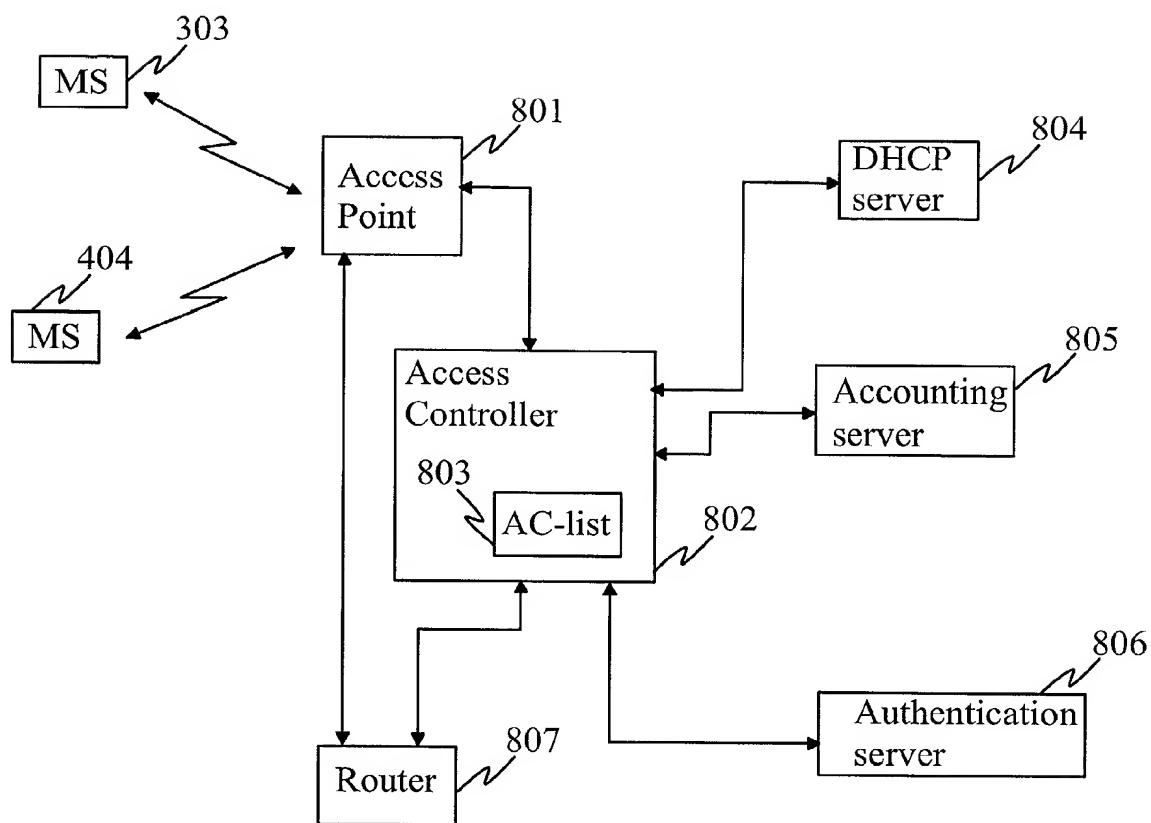


Fig. 8



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 02 25 0352

DOCUMENTS CONSIDERED TO BE RELEVANT			CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	
X	US 2001/001268 A1 (DOI NOBUKAZU ET AL) 5 April 2001 (2001-04-05)	1-9	H04L12/28 H04Q7/38 H04Q7/22
Y	* abstract *	11-15	
A	* page 2, paragraph 50 - page 3, paragraph 61; figures 1,5 *	16-33	
	* page 4, paragraph 79 *		
	* page 5, paragraph 84 *		
	* page 9, paragraph 141 *		
	* page 19, paragraph 285 *		
	* page 20, paragraph 287 - paragraph 289 *		
	* page 25, paragraph 363 *		
Y	WO 01 41470 A (QUALCOMM INC) 7 June 2001 (2001-06-07)	11-15	
A	* abstract; figure 5 *	16-33	
	* page 3, line 20 - line 37 *		
	* page 4, line 32 - page 6, line 15; figure 1 *		
	* page 7, line 34 - line 36 *		
A	WO 00 76249 A (ERICSSON TELEFON AB L M) 14 December 2000 (2000-12-14)	1-33	TECHNICAL FIELDS SEARCHED (Int.Cl.7)
	* abstract; figures 1,2 *		H04L
	* page 2, line 1 - line 14 *		H04Q
<p>The present search report has been drawn up for all claims</p>			
Place of search	Date of completion of the search	Examiner	
MUNICH	30 August 2002	Hultsch, W	
CATEGORY OF CITED DOCUMENTS			
X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document			
T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document			



European Patent
Office

Application Number

CLAIMS INCURRING FEES

The present European patent application comprised at the time of filing more than ten claims.

Only part of the claims have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims and for those claims for which claims fees have been paid, namely claim(s):

No claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims.

LACK OF UNITY OF INVENTION

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

see sheet B

All further search fees have been paid within the fixed time limit. The present European search report has been drawn up for all claims.

As all searchable claims could be searched without effort justifying an additional fee, the Search Division did not invite payment of any additional fee.

Only part of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the inventions in respect of which search fees have been paid, namely claims:

None of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims, namely claims:



The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

1. Claims: 1-15

Method for relaying data packets of a terminal device in a communication network and a related access point for setting up a communication connection to a terminal device in a network.

2. Claims: 16-33

Method and a system for access control of a terminal device in a communication network and a related access point for setting up a communication connection to a terminal device in a network.

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 02 25 0352

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on.
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

30-08-2002

Patent document cited in search report		Publication date		Patent family member(s)	Publication date
US 2001001268	A1	17-05-2001	CN EP WO US US	1350741 T 1142266 A1 0038391 A1 2001022784 A1 2002048268 A1	22-05-2002 10-10-2001 29-06-2000 20-09-2001 25-04-2002
WO 0141470	A	07-06-2001	AU WO	1815701 A 0141470 A2	12-06-2001 07-06-2001
WO 0076249	A	14-12-2000	GB AU EP WO GB	2350970 A 5435600 A 1183894 A1 0076249 A1 2350975 A	13-12-2000 28-12-2000 06-03-2002 14-12-2000 13-12-2000

PUB-NO: EP001330073A1
DOCUMENT-IDENTIFIER: EP 1330073 A1
TITLE: Method and apparatus for access control of a wireless terminal device in a communications network
PUBN-DATE: July 23, 2003

INVENTOR-INFORMATION:

NAME	COUNTRY
HAVERINEN, HENRY	FI
BUSH, ANTON	GB
RINNEMAA, JYRI	FI
SMITH, MIKE P	GB
TAKAMAEKI, TIMO	FI
TUOMI, JUKKA	FI
TUOMINEN, HANNU	FI

ASSIGNEE-INFORMATION:

NAME	COUNTRY
NOKIA CORP	FI

APPL-NO: EP02250352
APPL-DATE: January 18, 2002

PRIORITY-DATA: EP02250352A (January 18, 2002)

INT-CL (IPC) : H04L012/28 , H04Q007/38 ,
H04Q007/22

EUR-CL (EPC) : H04L012/28 , H04L012/56 ,
H04L029/06 , H04L029/12 ,
H04L029/12 , H04W006/06 ,
H04W036/08

ABSTRACT:

CHG DATE=20030902 STATUS=O> A method and device for routing data packets (110) of a wireless terminal device in a communication network. When Open system Authentication is used (103) the system operates similarly as the current Nokia Operator Wireless LAN system, in which the terminal device and the access controller are the parties involved in the authentication (105). The access controller relays information relating to the authentication between the terminal device and an authenticating server, and it is capable of updating independently the list of users it maintains. When authentication according IEEE 802.1X authentication (102), the access point operates according to the IEEE 802.1X standard (108), serving as the authenticating party and relaying information relating to the authentication between the terminal device and the authentication server. In addition, the list maintained by the access controller is updated (107) after a successful authentication, for example by the access point or the authenticating server. ?